

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for enabling an identity change
2 during a certificate-based host access session, said computer program product embodied on a
3 computer-readable medium and comprising:

4 computer-readable program code means for processing a first sign-on during a secure
5 session using a digital certificate, further comprising:

6 computer-readable program code means for establishing said secure session from a
7 client machine to a server machine using said digital certificate, wherein said digital certificate
8 represents an identity of said client machine or a user thereof;

9 computer-readable program code means for storing said digital certificate or a
10 reference thereto at said server machine;

11 computer-readable program code means for establishing a session from said server
12 machine to a host system using a legacy host communication protocol, responsive to receiving, at
13 said server machine, a first sign-on request from said client machine, wherein said first sign-on
14 request identifies a first secure legacy host application to which said first sign-on is requested;

15 computer-readable program code means for passing said stored digital certificate
16 or said reference from said server machine to a host access security system;

17 computer-readable program code means, operable in said host access security
18 system, for authenticating said identity using said passed digital certificate or a retrieved
19 certificate which is retrieved using said reference;

20 computer-readable program code means, operable in said host access security
21 system, for using said passed or retrieved digital certificate to locate access credentials for said

Serial No. 09/619,912

-7-

Docket RSW9-2000-0081-US1

22 user;

23 computer-readable program code means, operable in said host access security
24 system, for accessing a stored password or generating a password substitute representing said
25 located credentials;

26 computer-readable program code means, operable in said host access security
27 system, for returning said stored password or generated password substitute to said server
28 machine, along with a first user identifier corresponding to said located credentials; and

29 computer-readable program code means, operable in said server machine, for using
30 said returned stored password or said generated password substitute and said returned first user
31 identifier to transparently complete said first sign-on, on behalf of said user of said client machine,
32 to [[a]] said first secure legacy host application executing at said host system; and

33 computer-readable program code means for processing a second sign-on during said
34 secure session, without requiring establishment of a new secure session between said client
35 machine and said server machine, using a second digital certificate [[for]] that represents a second
36 identity, wherein said second sign-on requests access to said secure legacy host application or a
37 different legacy host application by said user or by a different user, further comprising:

38 computer-readable program code means for receiving a second sign-on request, at
39 said server machine from said client machine, wherein: (1) said second sign-on request identifies
40 a second secure legacy host application to which said second sign-on is requested; (2) said second
41 sign-on request includes [[using]] said second digital certificate, or a second certificate reference
42 that references said second digital certificate, for said second identity; (3) said second secure
43 legacy host application may be identical to said first secure legacy host application; and (4) said

Serial No. 09/619,912

-8-

Docket RSW9-2000-0081-US1

44 second identity is for a second user, wherein said second user may be identical to said user;

45 computer-readable program code means for passing said second digital certificate
46 or [[a]] said second certificate reference from said server machine to said host access security
47 system;

48 computer-readable program code means, operable in said host access security
49 system, for authenticating said second identity using said passed second digital certificate or a
50 second retrieved certificate which is retrieved using said second certificate reference;

51 computer-readable program code means, operable in said host access security
52 system, for using said passed second digital certificate or said second retrieved certificate to
53 locate second access credentials for said second user;

54 computer-readable program code means, operable in said host access security
55 system, for accessing a second stored password or generating a second password substitute
56 representing said second located credentials;

57 computer-readable program code means, operable in said host access security
58 system, for returning said second stored password or second generated password substitute to
59 said server machine, along with a second user identifier corresponding to said second located
60 credentials; and

61 computer-readable program code means, operable in said server machine, for using
62 said returned second stored password or [[said]] second password substitute and said returned
63 second user identifier to transparently complete said second sign-on, on behalf of said second user
64 of said client machine, to said second secure legacy host application executing at said host system
65 or said different legacy host application.

Serial No. 09/619,912

-9-

Docket RSW9-2000-0081-US1

1 Claim 2 (currently amended): The computer program product as claimed in Claim 1, wherein said
2 digital certificate ~~[[is an]]~~ and said second digital certificate are X.509 certificate certificates and
3 said digital certificate reference and second certificate reference are references to an X.509
4 certificate.

1 Claim 3 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a 3270 emulation protocol.

27
1 Claim 4 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a 5250 emulation protocol.

1 Claim 5 (original): The computer program product as claimed in Claim 1, wherein said
2 communication protocol is a Virtual Terminal protocol.

1 Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host
2 access security system is a Resource Access Control Facility (RACF) system.

1 Claim 7 (currently amended): The computer program product as claimed in Claim 1, wherein said
2 computer-readable program code means for processing said second sign-on further comprises
3 computer-readable program code means for storing said second digital certificate at said server
4 machine.

Serial No. 09/619,912

-10-

Docket RSW9-2000-0081-US1

1 Claim 8 (currently amended): The computer program product as claimed in Claim 1, wherein:

2 said computer-readable program code means for processing said first sign-on further
3 comprises:

4 computer-readable program code means for requesting by said first secure legacy
5 host application, responsive to said computer-readable program code means for establishing said
6 session, first sign-on information for said user; and

7 computer-readable program code means for responding to said request for first
8 sign-on information by sending a first sign-on message with placeholders from said client machine
9 to said server machine, said placeholders representing a user identification and a password of said
10 user; and

11 said computer-readable program code means for using said returned password or
12 password substitute and said returned first user identifier to transparently complete said first sign-
13 on further comprises:

14 computer-readable program code means for substituting [[a]] said returned user
15 identifier ~~associated with said located access credentials~~ and said stored returned password or said
16 generated password substitute for said placeholders in said first sign-on message, thereby creating
17 a revised first sign-on message; and

18 computer-readable program code means for forwarding said revised first sign-on
19 message from said server machine to said first secure legacy host application.

20 ~~— said computer-readable program code means for processing said second sign-on further~~
21 ~~comprises:~~

Serial No. 09/619,912

-11-

Docket RSW9-2000-0081-US1

22 ~~computer-readable program code means for requesting, by said legacy host~~
23 ~~application, second sign-on information for said second identity,~~
24 ~~computer-readable program code means for responding to said request for second~~
25 ~~sign-on information by sending a second sign-on message with placeholders from said client~~
26 ~~machine to said server machine, said placeholders representing a different user identification and a~~
27 ~~different password of said second identity, and~~
28 ~~computer-readable program code means for substituting said second user identifier~~
29 ~~associated with said second access credentials and said second stored password or said second~~
a7 30 ~~password substitute for said placeholders in said second sign-on message.~~

1 Claim 9 (currently amended): A system for enabling an identity change during a certificate-based
2 host access session, comprising:
3 means for processing a first sign-on during a secure session using a digital certificate,
4 further comprising:
5 means for establishing said secure session from a client machine to a server
6 machine using said digital certificate, wherein said digital certificate represents an identity of said
7 client machine or a user thereof,
8 means for storing said digital certificate or a reference thereto at said server
9 machine;
10 means for establishing a session from said server machine to a host system using a
11 legacy host communication protocol, responsive to receiving, at said server machine, a first sign-
12 on request from said client machine, wherein said first sign-on request identifies a first secure

13 legacy host application to which said first sign-on is requested;

14 means for passing said stored digital certificate or said reference from said server
15 machine to a host access security system;

16 means, operable in said host access security system, for authenticating said identity
17 using said passed digital certificate or a retrieved certificate which is retrieved using said
18 reference;

19 means, operable in said host access security system, for using said passed or
20 retrieved digital certificate to locate access credentials for said user;

a7 21 means, operable in said host access security system, for accessing a stored
22 password or generating a password substitute representing said located credentials;

23 means, operable in said host access security system, for returning said stored
24 password or generated password substitute to said server machine, along with a first user
25 identifier corresponding to said located credentials; and

26 means, operable in said server machine, for using said returned stored password or
27 said generated password substitute and said returned first user identifier to transparently complete
28 said first sign-on, on behalf of said user of said client machine, to [[a]] said first secure legacy host
29 application executing at said host system; and

30 means for processing a second sign-on during said secure session, without requiring
31 establishment of a new secure session between said client machine and said server machine, using
32 a second digital certificate [[for]] that represents a second identity, wherein said second sign-on
33 requests access to said secure legacy host application or a different legacy host application by said
34 user or by a different user, further comprising:

Serial No. 09/619,912

-13-

Docket RSW9-2000-0081-US1

35 means for receiving a second sign-on request, at said server machine from said
36 client machine, wherein: (1) said second sign-on request identifies a second secure legacy host
37 application to which said second sign-on is requested; (2) said second sign-on request includes
38 [[using]] said second digital certificate, or a second certificate reference that references said
39 second digital certificate, for said second identity; (3) said second secure legacy host application
40 may be identical to said first secure legacy host application; and (4) said second identity is for a
41 second user, wherein said second user may be identical to said user;

42 means for passing said second digital certificate or [[a]] said second certificate
43 reference from said server machine to said host access security system;

44 means, operable in said host access security system, for authenticating said second
45 identity using said passed second digital certificate or a second retrieved certificate which is
46 retrieved using said second certificate reference;

47 means, operable in said host access security system, for using said passed second
48 digital certificate or said second retrieved certificate to locate second access credentials for said
49 second user;

50 means, operable in said host access security system, for accessing a second stored
51 password or generating a second password substitute representing said second located
52 credentials;

53 means, operable in said host access security system, for returning said second
54 stored password or second generated password substitute to said server machine, along with a
55 second user identifier corresponding to said second located credentials; and

56 means, operable in said server machine, for using said returned second stored

57 password or [[said]] second password substitute and said returned second user identifier to
58 transparently complete said second sign-on, on behalf of said second user of said client machine,
59 to said second secure legacy host application executing at said host system ~~or said different legacy~~
60 ~~host application.~~

1 Claim 10 (currently amended): The system as claimed in Claim 9, wherein said digital certificate
2 and said second digital certificate are [[is an]] X.509 certificate certificates and said digital
3 certificate reference and second certificate reference are references to an X.509 certificate.

a7
1 Claim 11 (original): The system as claimed in Claim 9, wherein said communication protocol is a
2 3270 emulation protocol.

1 Claim 12 (original): The system as claimed in Claim 11, wherein said host access security system
2 is a Resource Access Control Facility (RACF) system.

1 Claim 13 (currently amended): The system as claimed in Claim 9, wherein said means for
2 processing said second sign-on further comprises means for storing said second digital certificate
3 at said server machine.

1 Claim 14 (currently amended): The system as claimed in Claim 9, wherein:
2 said means for processing said first sign-on further comprises:
3 means for requesting by said first secure legacy host application, responsive to said

Serial No. 09/619,912

-15-

Docket RSW9-2000-0081-US1

4 means for establishing said session, first sign-on information for said user; and

5 means for responding to said request for first sign-on information by sending a first
6 sign-on message with placeholders from said client machine to said server machine, said
7 placeholders representing a user identification and a password of said user; and

8 said means for using said returned password or password substitute and said returned first
9 user identifier to transparently complete said first sign-on further comprises:

10 means for substituting ~~[[a]]~~ said returned user identifier ~~associated with said~~
11 ~~located access credentials~~ and said stored returned password or ~~said generated~~ password
12 substitute for said placeholders in said first sign-on message, thereby creating a revised first sign-
13 on message; and

14 means for forwarding said revised first sign-on message from said server machine
15 to said first secure legacy host application.

16 ~~said means for processing said second sign-on further comprises:~~

17 ~~means for requesting, by said legacy host application, second sign-on information~~
18 ~~for said second identity,~~

19 ~~means for responding to said request for second sign-on information by sending a~~
20 ~~second sign-on message with placeholders from said client machine to said server machine, said~~
21 ~~placeholders representing a different user identification and a different password of said second~~
22 ~~identity; and~~

23 ~~means for substituting said second user identifier associated with said second~~
24 ~~access credentials and said second stored password or said second password substitute for said~~
25 ~~placeholders in said second sign-on message.~~

Serial No. 09/619,912

-16-

Docket RSW9-2000-0081-US1

1 Claim 15 (currently amended): A method for enabling an identity change during a certificate-
2 based host access session, comprising the steps of:

3 processing a first sign-on during a secure session using a digital certificate, further
4 comprising the steps of:

5 establishing said secure session from a client machine to a server machine using
6 said digital certificate, wherein said digital certificate represents an identity of said client machine
7 or a user thereof;

8 storing said digital certificate or a reference thereto at said server machine;

a7
9 establishing a session from said server machine to a host system using a legacy
10 host communication protocol, responsive to receiving, at said server machine, a first sign-on
11 request from said client machine, wherein said first sign-on request identifies a first secure legacy
12 host application to which said first sign-on is requested;

13 passing said stored digital certificate or said reference from said server machine to
14 a host access security system;

15 authenticating, by said host access security system, said identity using said passed
16 digital certificate or a retrieved certificate which is retrieved using said reference;

17 using, by said host access security system, said passed or retrieved digital
18 certificate to locate access credentials for said user;

19 accessing, by said host access security system, a stored password or generating a
20 password substitute representing said located credentials;

21 returning, by said host access security system, said stored password or generated

Serial No. 09/619,912

-17-

Docket RSW9-2000-0081-US1

22 password substitute to said server machine, along with a first user identifier corresponding to said
23 located credentials; and

24 using, by said server machine, said returned stored password or said-generated
25 password substitute and said returned first user identifier to transparently complete said first sign-
26 on, on behalf of said user of said client machine, to [[a]] said first secure legacy host application
27 executing at said host system; and

28 processing a second sign-on during said secure session, without requiring establishment of
29 a new secure session between said client machine and said server machine, using a second digital
30 certificate [[for]] that represents a second identity, wherein said second sign-on requests access to
31 said secure legacy host application or a different legacy host application by said user or by a
32 different user, further comprising the steps of:

33 receiving a second sign-on request, at said server machine from said client
34 machine, wherein: (1) said second sign-on request identifies a second secure legacy host
35 application to which said second sign-on is requested; (2) said second sign-on request includes
36 [[using]] said second digital certificate, or a second certificate reference that references said
37 second digital certificate, for said second identity; (3) said second secure legacy host application
38 may be identical to said first secure legacy host application; and (4) said second identity is for a
39 second user, wherein said second user may be identical to said user;

40 passing said second digital certificate or [[a]] said second certificate reference from
41 said server machine to said host access security system;

42 authenticating, by said host access security system, said second identity using said
43 passed second digital certificate or a second retrieved certificate which is retrieved using said

Serial No. 09/619,912

-18-

Docket RSW9-2000-0081-US1

44 second certificate reference;

45 using, by said host access security system, said passed second digital certificate or
46 said second retrieved certificate to locate second access credentials for said second user;

47 accessing, by said host access security system, a second stored password or
48 generating a second password substitute representing said second located credentials;

49 returning, by said host access security system, said second stored password or
50 second generated password substitute to said server machine, along with a second identifier
51 corresponding to said second located credentials; and

52 using, by said server machine, said returned second stored password or [[said]]
53 second password substitute and said returned second user identifier to transparently complete said
54 second sign-on, on behalf of said second user of said client machine, to said second secure legacy
55 host application executing at said host system or said different legacy host application.

1 Claim 16 (currently amended): The method as claimed in Claim 15, wherein said digital
2 certificate and said second digital certificate are [[is an]] X.509 certificate certificates and said
3 digital certificate reference and second certificate reference are references to an X.509 certificate.

1 Claim 17 (original): The method as claimed in Claim 15, wherein said communication protocol is
2 a 3270 emulation protocol.

1 Claim 18 (original): The method as claimed in Claim 17, wherein said host access security system
2 is a Resource Access Control Facility (RACF) system.

Serial No. 09/619,912

-19-

Docket RSW9-2000-0081-US1

1 Claim 19 (currently amended): The method as claimed in Claim 15, wherein said step of
2 processing said second sign-on further comprises the step of storing said second digital certificate
3 at said server machine.

1 Claim 20 (currently amended): The method as claimed in Claim 15, wherein:

2 said step of processing said first sign-on further comprises the steps of:

3 requesting by said first secure legacy host application, responsive to said step of
4 establishing said session, first sign-on information for said user; and

5 responding to said request for first sign-on information by sending a first sign-on
6 message with placeholders from said client machine to said server machine, said placeholders
7 representing a user identification and a password of said user; and

8 said step of using said returned password or password substitute and said returned first
9 user identifier to transparently complete said first sign-on further comprises the steps of:

10 substituting ~~[[a]]~~ said returned user identifier ~~associated with said located access~~
11 ~~credentials~~ and said returned stored password or said-generated password substitute for said
12 placeholders in said first sign-on message, thereby creating a revised first sign-on message; and
13 forwarding said revised first sign-on message from said server machine to said first
14 secure legacy host application.

15 said step of processing said second sign-on further comprises the steps of:

16 ~~requesting, by said legacy host application, second sign-on information for said~~
17 ~~second identity;~~

Serial No. 09/619,912

-20-

Docket RSW9-2000-0081-US1

18 ~~_____ responding to said request for second sign-on information by sending a second~~
19 ~~sign-on message with placeholders from said client machine to said server machine, said~~
20 ~~placeholders representing a different user identification and a different password of said second~~
21 ~~identity, and~~
22 ~~_____ substituting said second user identifier associated with said second access~~
23 ~~credentials and said second stored password or said second password substitute for said~~
24 ~~placeholders in said second sign-on message.~~

1 Claim 21 (new): The computer program product as claimed in Claim 1, wherein:

2 said computer-readable program code means for processing said second sign-on further
3 comprises computer-readable program code means for receiving, at said server machine, a second
4 sign-on message sent from said client machine, wherein said second sign-on message has
5 placeholders representing a user identification of said second user and a password of said second
6 user; and

7 said computer-readable program code means for using said returned second password or
8 second password substitute and said returned second user identifier to transparently complete said
9 second sign-on further comprises:

10 computer-readable program code means for substituting said returned second user
11 identifier and said returned second password or second password substitute for said placeholders
12 in said second sign-on message, thereby creating a revised second sign-on message; and

13 computer-readable program code means for forwarding said revised second sign-
14 on message from said server machine to said second secure legacy host application.

1 Claim 22 (new): The computer program product according to Claim 1, wherein said second sign-
2 on request includes information usable as proof that said second user owns said second digital
3 certificate.

1 Claim 23 (new): The computer program product according to Claim 22, wherein said proof
2 further comprises a random seed value and a sequence number concatenated thereto by said client
3 machine to detect replay attacks, wherein said random seed value was previously sent from said
4 server machine to said client machine.

27
1 Claim 24 (new): The computer program product according to Claim 23, wherein said
2 identification of said second secure legacy host application is also concatenated to said random
3 seed value.

1 Claim 25 (new): The computer program product according to Claim 23, wherein a digital
2 signature computed using a private key associated with said second digital certificate is included
3 in said second sign-on request, said digital signature covering said random seed value and said
4 concatenated sequence number.

1 Claim 26 (new): The computer program product according to Claim 24, wherein a digital
2 signature computed using a private key associated with said second digital certificate is included
3 in said second sign-on request, said digital signature covering said random seed value, said

Serial No. 09/619,912

-22-

Docket RSW9-2000-0081-US1

4 concatenated sequence number, and said concatenated identification of said second secure legacy
5 host application.

1 Claim 27 (new): The system as claimed in Claim 9, wherein:

2 said means for processing said second sign-on further comprises means for receiving, at
3 said server machine, a second sign-on message sent from said client machine, wherein said second
4 sign-on message has placeholders representing a user identification of said second user and a
5 password of said second user; and

6 said means for using said returned second password or second password substitute and
7 said returned second user identifier to transparently complete said second sign-on further
8 comprises:

9 means for substituting said returned second user identifier and said returned
10 second password or second password substitute for said placeholders in said second sign-on
11 message, thereby creating a revised second sign-on message; and

12 means for forwarding said revised second sign-on message from said server
13 machine to said second secure legacy host application.

1 Claim 28 (new): The method as claimed in Claim 15, wherein:

2 said step of processing said second sign-on further comprises the step of receiving, at said
3 server machine, a second sign-on message sent from said client machine, wherein said second
4 sign-on message has placeholders representing a user identification of said second user and a
5 password of said second user; and

Serial No. 09/619,912

-23-

Docket RSW9-2000-0081-US1

6 said step of using said returned second password or second password substitute and said
7 returned second user identifier to transparently complete said second sign-on further comprises
8 the steps of:

9 substituting said returned second user identifier and said returned second password
10 or second password substitute for said placeholders in said second sign-on message, thereby
11 creating a revised second sign-on message; and
12 forwarding said revised second sign-on message from said server machine to said
13 second secure legacy host application.

1 Claim 29 (new): A computer-implemented method for enabling an identity change during a
2 certificate-based host access session, comprising steps of:

3 establishing a secure session between a client and a server using a digital certificate owned
4 by a user of said client;

5 remembering said digital certificate at said server;

6 completing a first sign-on to a host application, by said server on behalf of said user,
7 responsive to receiving an asynchronous sign-on request from said client that identifies said host
8 application, further comprising the steps of:

9 using said remembered digital certificate to authenticate said user to a host access
10 security component;

11 if said user is authenticated, locating, by said host access security component,
12 access credentials of said user;

13 creating, by said host access security component, a passticket that represents said

Serial No. 09/619,912

-24-

Docket RSW9-2000-0081-US1

14 located access credentials;
15 returning said passticket from said host access security component to said server,
16 along with a user identifier associated with said located access credentials; and
17 inserting, by said server, said passticket and said user identifier into a log-on
18 message in place of placeholders therefor, when said log-on message is received at said server
19 from said client, thereby creating a revised log-on message that is then sent from said server to
20 sign said user on to said host application; and
21 completing a second sign-on to a second host application, by said server on behalf of a
22 second user, responsive to receiving a second asynchronous sign-on request from said client that
23 identifies said second host application, wherein said second host application may be identical to
24 said host application and said second user may be identical to said user, further comprising the
25 steps of:
26 using a new digital certificate and proof therefor to authenticate said second user
27 to said host access security component, wherein said new digital certificate and said proof
28 therefor are included in said second asynchronous sign-on request;
29 if said second user is authenticated, locating, by said host access security
30 component, access credentials of said second user;
31 creating, by said host access security component, a second passticket that
32 represents said located access credentials of said second user;
33 returning said second passticket from said host access security component to said
34 server, along with a second user identifier associated with said located access credentials of said
35 second user; and

Serial No. 09/619,912

-25-

Docket RSW9-2000-0081-US1

36 inserting, by said server, said returned second passticket and said returned second
37 user identifier into a second log-on message in place of placeholders therefor, when said second
38 log-on message is received at said server from said client, thereby creating a revised second log-
39 on message that is then sent from said server to sign said second user on to said second host
40 application.

Serial No. 09/619,912

-26-

Docket RSW9-2000-0081-US1